



# UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**  
**United States Patent and Trademark Office**  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,017	07/25/2003	John Mendonca	200209600-1	3688
22879 7590 07/12/2007 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			EXAMINER OKORONKWO, CHINWENDU C	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 07/12/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

**Application No.**

10/627,017

**Applicant(s)**

MENDONCA ET AL.

**Examiner**

Chinwendu C. Okoronkwo

**Art Unit**

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 04/16/2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### *Response to Remarks/Arguments*

1. In response to communications filed on 04/16/2007. The following claims, claims 1-20, are presented for examination.

1.1 Applicant's arguments, pages 2-5, with respect to the rejection of claims 1-20 have been fully considered but they are not persuasive.

1.2 In response to Applicant argument that the Shanklin et al. reference does not teach or suggest said network intrusion detection systems in said dynamic data center receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy, the Examiner respectfully disagrees citing column 1 lines 37-48 and 64-66, which specifically recites, "signatures are stored, and in real time, compared to the packet flow incoming to the network" and "a plurality of intrusion detection sensors ... connected at a network entry point associated with an internetworking device." This disclosure of "signatures" is analogous to the claimed monitoring policy, as these signatures determine which datastream is determined a threat and which is not. The disclosure of these comparisons taking place in "real time" is analogous in functionality to the claimed "dynamic" factor of the data center claimed within the instant application. Further the disclosed "intrusion detection sensors" in

Art Unit: 2136

combination with the later disclosure of a "internetworking device ... [which] is processor-based and includes load balancing programming, which controls how packets are distributed from the internetworking device to the sensors for processing (column 2 lines 53-57)," essentially filters/monitors the data passing in and out of a network, which reads on the claimed "data center."

1.3 In response to Applicant argument that the Shanklin et al. reference does not teach or suggest a "plurality of entry points" which can be monitored with any network, the Examiner respectfully disagrees citing column 1 lines 64-66 which recite, specifically "a plurality of intrusion detection sensors ... connected at a network entry point associated with an internetworking device" and column 2 lines 13-17, which recites, "a processor-based intrusion detection system that can keep up with the high traffic throughput of today's networks. Existing sensors may be used, and the solution provided by the invention is easily scalable." The disclosed scalability of the invention reads upon the claims of monitoring on "any" network.

### ***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Art Unit: 2136

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being disclosed by Shanklin et al. (U.S. Patent No. 6578147 B1).

Regarding claim 1, Shanklin et al., discloses a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center; receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy (col. 1 lines 63-67 and col. 2 lines 1-18).

Regarding claim 2, Shanklin et al., discloses the method as recited in claim 1

wherein said automatically arranging the monitoring of said monitoring points includes: automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy (col. 4 lines 43-67 and col. 5 lines 1-11).

Regarding claim 3, Shanklin et al., discloses the method as recited in claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically increasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (col. 5 lines 14-67 and col. 6 lines 1-55).

Regarding claim 4, Shanklin et al., discloses the method as recited in claim 2 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said

network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems (col. 5 lines 14-67 and col. 6 lines 1-55).

Regarding claim 5, Shanklin et al., discloses the method as recited in claim 2 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router (col. 6 lines 58-67 and col. 7 lines 1-38).

Regarding claim 6, Shanklin et al., discloses the method as recited in claim 1 wherein said receiving a monitoring policy and a plurality of monitoring points to be monitored includes: providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored (col. 3 lines 54-65).

Regarding claim 7, Shanklin et al., discloses the method as recited in claim 1 wherein said dynamic data center is a utility data center (col. 1 lines 63-67 and col. 2 lines 1-18).

Regarding claim 8, Shanklin et al., discloses a computer-readable medium comprising computer-executable instructions stored therein for performing a method of managing utilization of network intrusion detection systems in a dynamic data center, said method comprising: providing a plurality of network

Art Unit: 2136

intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center; receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy (Rejected under the same rationale as claim 1).

Regarding claim 9, Shanklin et al., discloses the computer-readable medium as recited in claim 8 wherein said automatically arranging the monitoring of said monitoring points includes: automatically configuring a plurality of network resources to provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems; and automatically configuring said available network intrusion detection systems to receive said network communication data based on said monitoring policy (Rejected under the same rationale as claim 2).

Regarding claim 10, Shanklin et al., discloses the computer-readable medium as recited in claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically increasing a number of particular network intrusion detection systems receiving said network communication data



from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 3).

Regarding claim 11, Shanklin et al., discloses the computer-readable medium as recited in claim 9 wherein said automatically arranging the monitoring of said monitoring points further includes: automatically decreasing a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 4).

Regarding claim 12, Shanklin et al., discloses the computer-readable medium as recited in claim 9 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router (Rejected under the same rationale as claim 5).

Regarding claim 13, Shanklin et al., discloses the computer-readable medium as recited in claim 8 wherein said receiving a monitoring policy and a plurality of

monitoring points to be monitored includes: providing a graphical user interface to receive said monitoring policy and said plurality of monitoring points to be monitored (Rejected under the same rationale as claim 6).

Regarding claim 14, Shanklin et al., discloses the computer-readable medium as recited in claim 8 wherein said dynamic data center is a utility data center (Rejected under the same rationale as claim 7).

Regarding claim 15, Shanklin et al., discloses the system comprising: a dynamic data center including: a plurality of network resources; a plurality of network intrusion detection systems, each being networked so that utilization of each network intrusion detection system can be based on demand for said network intrusion detection systems in said dynamic data center; a graphical user interface for receiving a monitoring policy and a plurality of monitoring points to be monitored on a network with any of said network intrusion detection systems; and a controller for controlling said network resources and said network intrusion detection systems and for automatically arranging the monitoring of said monitoring points using said network intrusion detection systems and said monitoring policy (Rejected under the same rationale as claim 1).

Regarding claim 16, Shanklin et al., discloses the system as recited in claim 15 wherein said controller automatically configures said network resources to

provide network communication data from said monitoring points to a plurality of available network intrusion detection systems from said network intrusion detection systems, and wherein said controller automatically configures said available network intrusion detection systems to receive said network communication data based on said monitoring policy (Rejected under the same rationale as claim 2).

Regarding claim 17, Shanklin et al., discloses the system as recited in claim 16 wherein said controller automatically increases a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by selecting additional available network intrusion detection systems if said network communication data exceeds a capacity of said particular network intrusion detection systems (Rejected under the same rationale as claim 3).

Regarding claim 18, Shanklin et al., discloses the system as recited in claim 16 wherein said controller automatically decreases a number of particular network intrusion detection systems receiving said network communication data from a particular monitoring point by releasing any of said particular network intrusion detection systems to said available network intrusion detection systems if said network communication data is below a predetermined threshold of a capacity of

Art Unit: 2136

said particular network intrusion detection systems (Rejected under the same rationale as claim 4).

Regarding claim 19, Shanklin et al., discloses the system as recited in claim 15 wherein said network resources include one of a firewall, a gateway system, a network switch, and a network router (Rejected under the same rationale as claim 5).

Regarding claim 20, Shanklin et al., discloses the system as recited in claim 15 wherein said dynamic data center is a utility data center (Rejected under the same rationale as claim 7).

***Conclusion***

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



CCO

July 5, 2007

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100



7,6,07